The Digital Arms Race: NSA Preps America for Future Ba

By Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marc Hilmar Schmundt and Michael Sontheimer

The NSA's mass surveillance is just the beginning. Documents from Edward Snowden sh intelligence agency is arming America for future digital wars -- a struggle for control of already well underway.

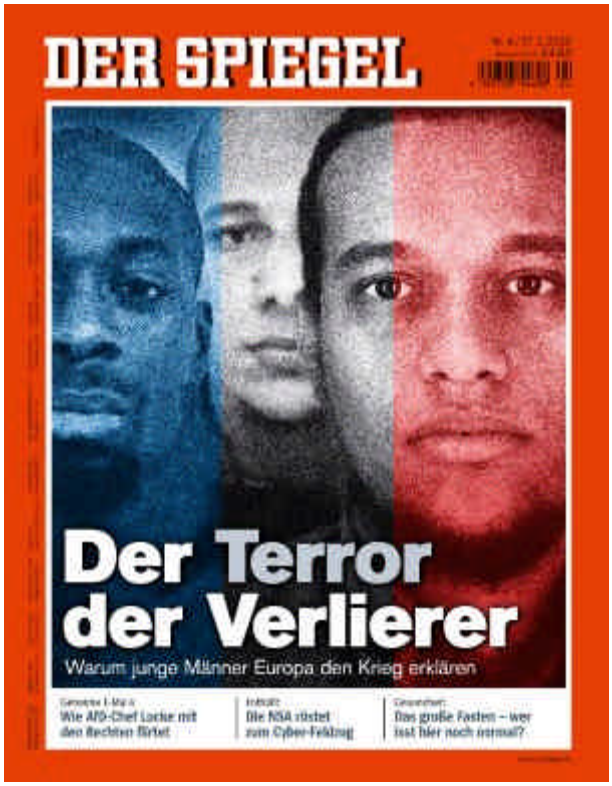
January 17, 2015 – 05:07 PM

Print | E-Mail

Feedback

Comment

From DER SPIEGEL



The article you are reading originally appeared in German in issue 4/2015 (January 17, 2015) of DER SPIEGEL.

Click on the links below for more information about DER SPIEGEL's history, how to subscribe or purchase the latest issue of the German-language edition in print or digital form or how to obtain rights to reprint SPIEGEL articles.

Frequently Asked Questions: Everything You Need to Know about DER SPIEGEL

Six Decades of Quality Journalism: The History of DER SPIEGEL

A New Home in HafenCity: SPIEGEL's New Hamburg HQ

Reprints: How To License SPIEGEL Articles

NSA Spying Scandal

National Security Agency

Government Communications Headquarters

Data Protection

are, the ad says, "looking for interns who want to

Politerain is not a project associated with a conventional company. It is run by a US government intelligence organization, the National Security Agency (NSA). More precisely, it's operated by the NSA's digital snipers with Tailored Access Operations (TAO), the department responsible for breaking into computers.

Potential interns are also told that research into third party computers might include plans to "remotely degrade or destroy op routers, servers and network enabled devices by hardware." Using a program called Passionatepol may be asked to "remotely brick network cards." Berserkr they would implant "persistent backdoo drivers". Using another piece of software called B "erase the BIOS on a brand of servers that act as rival governments."

An intern's tasks might also include remotely des of hard drives. Ultimately, the goal of the internsl "developing an attacker's mindset."

The internship listing is eight years old, but the a since become a kind of doctrine for the NSA's dat intelligence service isn't just trying to achieve ma Internet communication, either. The digital spies -- comprised of the United States, Britain, Canad Zealand -- want more.

The Birth of D Weapons

According to top secret documents from the archi Edward Snowden seen exclusively by SPIEGEL, th wars of the future in which the Internet will play a aim of being able to use the net to paralyze comp doing so, potentially all the infrastructure they co and water supplies, factories, airports or the flow

During the 20th century, scientists developed so- atomic, biological and chemical. It took decades could be regulated and, at least partly, outlawed.

Photo Gallery



Photo Gallery: What the Intelligence Agencies Can and Cannot Do

SPIEGEL's Top NSA Reports

DPA/ NSA

Prying Eyes: Inside the NSA's War on Internet Security

Obama's Lists: A Dubious History of Targeted Killings in Afghanistan

Spying Together: Germany's Deep Cooperation with the NSA

The NSA in Germany: Snowden's Documents Available for Download

New NSA Revelations: Inside Snowden's Germany File

'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel

NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need

Inside TAO: Documents Reveal Top NSA Hacking Unit

Friendly Fire: How GCHQ Monitors Germany, Israel and the EU

Embassy Espionage: The NSA's Secret Spy Hub in Berlin

iSpy: How the NSA Accesses Smartphone Data

Codename 'Apalachee': How America Spies on Europe and the UN

Cover Story: How the NSA Targets Germany and Europe

Related SPIEGEL ONLINE links

have now been developed for the war on the Inte
almost no international conventions or supervisor
weapons, and the only law that applies is the sur

Canadian media theorist Marshall McLuhan foresa
decades ago. In 1970, he wrote, "World War III is
war with no division between military and civilian
precisely the reality that spies are preparing for t

The US Army, Navy, Marines and Air Force have a
own cyber forces, but it is the NSA, also officially
is taking the lead. It's no coincidence that the dir
serves as the head of the US Cyber Command. Th
data spy, Admiral Michael Rogers, is also its chief
close to 40,000 employees are responsible for bo
destructive network attacks.

Surveillance only 'Phase 0'

From a military perspective, surveillance of the In
0" in the US digital war strategy. Internal NSA do
is the prerequisite for everything that follows. Th
the surveillance is to detect vulnerabilities in ene
"stealthy implants" have been placed to infiltrate
allowing "permanent accesses," then Phase Three
a phase headed by the word "dominate" in the do
them to "control/destroy critical systems & netwo
pre-positioned accesses (laid in Phase 0)." Critica
considered by the agency to be anything that is in
society running: energy, communications and tra
documents state that the ultimate goal is "real ti
escalation".

One NSA presentation proclaims that "the next m
cyberspace." To that end, the US government is c
massive effort to digitally arm itself for network w
secret intelligence budget, the NSA projected it w
billion in order to increase the strength of its com
operations. The budget included an increase of so
"unconventional solutions" alone.

NSA Docs on Network Attacks and Explo

**Excerpt from the secret NSA budget on computer n
word GENIE**

**Document about the expansion of the Remote Oper
endpoint operations**

Document explaining the role of the Remote Operat

Prying Eyes: Inside the NSA's War on Internet Security (12/28/2014)

NSA Documents: Attacks on VPN, SSL, TLS, SSH, Tor (12/28/2014)

Obama's Lists: A Dubious History of Targeted Killings in Afghanistan (12/28/2014)

Inside TAO: Documents Reveal Top NSA Hacking Unit (12/29/2013)

Interview with an employee of NSA's department f Operations about his field of work

Supply-chain interdiction / Stealthy techniques car hardest targets

Classification guide for computer network exploitat

NSA training course material on computer network

Overview of methods for NSA integrated cyber ope

NSA project description to recognize and process d party attacks on computers

Exploring and exploiting leaky mobile apps with BA

Overview of projects of the TAO/ATO department s destruction of network cards

iPhone target analysis and exploitation with Apple' identifiers (UDID)

Report of an NSA Employee about a Backdoor in the

NSA document on QUANTUMSHOOTER, an implant t computers with good network connections from un

In recent years, malware has emerged that expe the NSA and its Five Eyes alliance based on a nur include programs like Stuxnet, used to attack the program. Or Regin, a powerful spyware trojan th Germany after it infected the USB stick of a high- Chancellor Angela Merkel. Agents also used Regi European Commission, the EU's executive, and B company Belgacom in 2011.

Given that spies can routinely break through just software, virtually all Internet users are at risk of

The new documents shed some new light on othe Although an attack called Quantuminsert has bee SPIEGEL and others, documentation shows that i success rate and it has likely been replaced by m as Quantumdirk, which injects malicious content provided by websites such as Facebook and Yaho infected with Straitbizarre can be turned into disp non-attributable "shooter" nodes. These nodes ca messages from the NSA's Quantum network, whi and control for very large scale active exploitatio secret agents were also able to breach mobile ph vulnerability in the Safari browser in order to obt remotely implant malicious code.

In this guerilla war over data, little differentiatior soldiers and civilians, the Snowden documents sh

Twitter

could suffer damage to his or her data or comput potential to create perils in the offline world as w weapon like Barnfire were to destroy or "brick" th hospital as a result of a programming error, peop mobile phone could be affected.

Intelligence agencies have adopted "plausible de guiding principle for Internet operations. To ensu they seek to make it impossible to trace the auth

It's a stunning approach with which the digital sp undermine the very foundations of the rule of law approach threatens to transform the Internet into superpowers and their secret services operate ac whims with very few ways to hold them accounta

NSA Docs on Malware and Implants

CSEC document about the recognition of trojans an anomaly"

The formalized process through which analysts cho requirement and then get to know the tools that ca

QUANTUMTHEORY is a set of technologies allowing interference attacks on TCP/IP connections (includ and DAREDEVIL)

Sample code of a malware program from the Five E

Attribution is difficult and requires considerable fo new documents there are at least a few pointers. a keylogger that was part of the Snowden archive software designed to surreptitiously intercept all by the victim and record them for later inspection indeed rather dated, keylogger. Similar software numerous applications, so it doesn't seem to pos but the sourcecode contained in it does reveal so They suggest that this keylogger might be part of modules that that belong to the Warriorpride prog Esperanto software used by all the Five Eyes part times was even able to break into iPhones, amon documents published by SPIEGEL include sample keylogger to foster further research and enable t appropriate defenses.

'Just a Bunch of Hackers'

The men and women working for the Remote Op which uses the codename S321, at the agency's Meade, Maryland, work on one of the NSA's most

responsible for covert operations. S321 employee
third floor of one of the main buildings on the NS/
report from the Snowden archive, an NSA man re
when they got started, the ROC people were "jus
Initially, people worked "in a more ad hoc manne
Nowadays, however, procedures are "more syste
management massively expanded the ROC group
2005, the department's motto was, "Your data is
equipment is our equipment."

NSA Docs on Exfiltration

**Explanation of the APEX method of combining pass
methods to exfiltrate data from networks attacked**

**Explanation of APEX shaping to put exfiltrating net
patterns that allow plausible deniability**

**Presentation on the FASHIONCLEFT protocol that th
exfiltrate data from trojans and implants to the NS/**

**Methods to exfiltrate data even from devices which
offline**

**Document detailing SPINALTAP, an NSA project to
active operations and passive signals intelligence**

**Technical description of the FASHIONCLEFT protocc
exfiltrate data from Trojans and implants to the NS**

The agents sit in front of their monitors, working
clock. Just how close the NSA has already gotten
network dominance" is illustrated particularly wel
department S31177, codenamed Transgression.

The department's task is to trace foreign cyber at
analyze them and, in the best case scenario, to s
competing intelligence agencies. This form of "Cy
Intelligence" counts among the most delicate forr

Part 1: NSA Preps America for Future Battle

Part 2: How the NSA Reads Over Shoulders of Other Spie

Article...

Pri

Comments

Discuss this issue with other readers!

Share your opinion!

Share your thoughts

Please register to add a comment.

Subject optional

Comment

Keep track of the news

Stay informed with our free news services:

All news from SPIEGEL International

All news from World section

MORE FROM SPIEGEL INTERNATIONAL

GERMAN POLITICS

Merkel's Moves: Power Struggles in Berlin

WORLD WAR II

Truth and Reconciliation: Why the War Still Haunts Europe

ENERGY

Green Power: The Future of Energy

EUROPEAN UNION

United Europe: A Continental Project

OVERVI